(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 July 2004 (29.07.2004)

PCT

(10) International Publication Number
WO 2004/064011 A3

(51) International Patent Classification[7]: G06F 7/72

(21) International Application Number:
PCT/IB2003/006267

(22) International Filing Date:
19 December 2003 (19.12.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03100032.6 10 January 2003 (10.01.2003) EP

(71) Applicant *(for DE only)*: **PHILIPS INTELLECTUAL PROPERTY & STANDARDS GMBH** [DE/DE]; Steindamm 94, 20099 Hamburg (DE).

(71) Applicant *(for all designated States except DE, US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **WENG, Annegret** [DE/DE]; c/o Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen (DE).

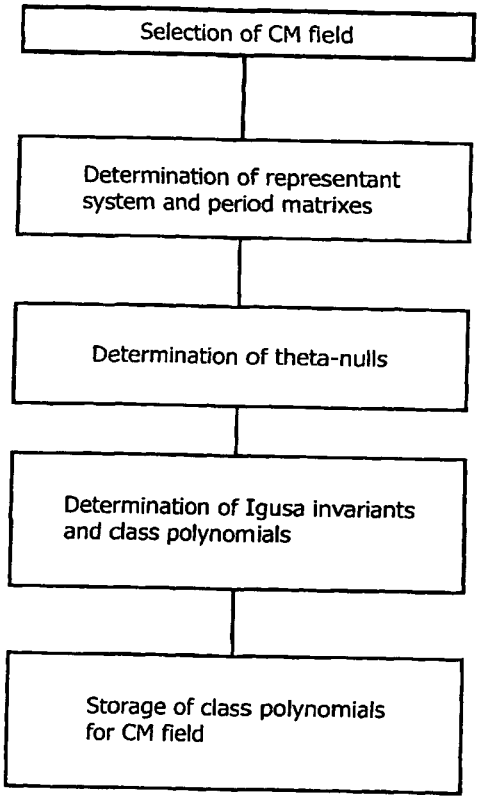
(74) Agent: **MEYER, Michael**; Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen (DE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE,

*[Continued on next page]*

(54) Title: METHOD OF CONSTRUCTING HYPERELLIPTIC CURVES SUITABLE FOR CRYPTOGRAPHIC PURPOSES AND CRYPTOGRAPHIC APPARATUS USING SUCH A METHOD




(57) Abstract: To provide a method for determining secure hyperelliptic curves quickly, it is proposed that suitable hyperelliptic curves be constructed using the complex multiplication method. The inventive method generates hyperelliptic curves, suitable for cryptographic applications, of genus 2 over finite fields having large characteristics. The invention further provides a cryptographic apparatus making use of a method as described beforehand can advantageously be used for encrypting and decrypting of messages for the secure exchange of information over public networks between senders and receivers. With such a cryptographic apparatus, messages and documents due for exchange can be encrypted fast and easily in an authentication procedure for the senders and receivers.

WO 2004/064011 A3

SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

**(88) Date of publication of the international search report:**
29 December 2004

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

# INTERNATIONAL SEARCH REPORT

In onal Application No
PCT/IB 03/06267

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | A. WENG: "Constructing Hyperelliptic curves of genus 2 suitable for cryptography" MATHEMATICS OF COMPUTATION, vol. 72, no. 241, 3 May 2002 (2002-05-03), pages 435-458, XP008038228 AMERICAN MATHEMATICAL SOCIETY, USA ISSN: 0025-5718 the whole document | 1-20 |

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 5 November 2004 | 19/11/2004 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Verhoof, P |